Contractor what additional information is required, and establish the date by which it should be furnished by the Contractor.

1.1 BACKGROUND

The Cybersecure Machinery Control Systems & Networks Department (NSWCPD Department 50) supports US Navy Machinery Controls, Navigation, Casualty Control, Conditioned-Based Maintenance, and Network Systems on all US Navy Surface Combatant, Amphibious, and Aircraft Carrier ships. NSWCPD Code 516 is the HM&E Controls Engineering Manager and Systems Integrator for all HM&E control systems, networks, and supporting systems.

1.2 SCOPE OF WORK

The work to be performed includes engineering support activities associated with HM&E controls for the Future Surface Combatant. HM&E controls includes the following areas (and will hereafter be referred to collectively as "HM&E Controls":

- Machinery Control System (MCS)
- Electric Plant Control System (EPCS)
- Propulsion Controls
- Auxiliary and Damage Control Embedded Controls/Controllers
- Ship Control Systems
- Navigation and Electronic Chart Systems
- Interior Communications Domain Networks (ICDN)
- Condition Based Monitoring (CBM)
- Data Acqusition Systems (DAS)
- Voyage Data Recorder (VDR)
- Digital Video Survelliance System (DVSS)
- HM&E sensors
- Common Display System (CDS) and Platform-as-a-Service (PaaS)

This includes program and financial tracking, cybersecurity, computer program development, hardware development, testing, Integrated Logistics Support (ILS), equipment troubleshooting, and installations on both in-service and new-ship-construction. Tasks include designing and developing new control systems, performing systems engineering analysis in order to interface HM&E control systems with other new or modified shipboard systems; troubleshooting control system hardware issues at Land Based Engineering Sites/Test Facilities in Philadelphia, PA; upgrading the cyber security features of the existing and future control system variants; addressing obsolete hardware with the most cost effective solutions possible.

2. APPLICABLE DOCUMENTS

Applicable documents and method of obtaining the documents are found below. The Contractor shall reference and utilize the latest version available when performing tasks within this SOW.

Documents can be found at https://quicksearch.dla.mil/qsSearch.aspx.

NAVSEA instructions can also be obtained by emailing navsea_instruc_nssc@navy.mil

2.1 DoD Documents

2.1.1 DoD 8140.01 Cyberspace Workforce Management requirement
2.1.2 DoD 8570.01 Risk Management Framework
2.1.3 DoD 8570.01-M Information Assurance Workforce Improvement Program

2.2 NAVSEA Instructions

2.2.1 NAVSEAINST 5400.111A, NAVSEA Engineering and Technical Authority Policy
2.2.2 NAVSEAINST S9800-AB-MAN-010, NAVSEA Engineering and Technical Authority Manual (ETAM)

2.3 MIL Standards

2.3.1 MIL-STD-480: Configuration Control - Engineering Changes, Deviations and Waivers
2.3.2 MIL-M-38784: Manuals, Technical: General Style and Format Requirements
2.3.3 MIL-P-24534: Planned Maintenance System: Development of Maintenance Requirement Cards, Maintenance Index Pages, and Associated Documentation

2.4 Miscellaneous

2.4.1 Joint Fleet Maintenance Manual (JFMM) –CINCLANT / CINCPACFLTINST 4790 (series)

3. REQUIREMENTS

3.1 Program Management Support: The contractor shall support the HM&E Controls Engineering Manager in providing program management support. This includes:

3.1.1 Tracking program spend rates and burn curves across all Future Surface Combatant HM&E control activities

3.1.2 Developing briefs and program documents

3.1.3 Participate in technical meetings and program reviews to provide action-item-tracking support and to draft meeting minutes.

3.1.4 Develop Plan of Actions and Milestones (POA&Ms) for initiatives, and provide status on the progress of those milestones.

3.1.5 Generate project plans, concepts of operation, and management outlines.

3.1.6 Develop and present technical presentations and information to various entities such as peers, shipboard installation managers, ship's force representatives, and program sponsors.

3.1.7 Develop and maintain tracking sheets for various types of work products, including test equipment tracking, purchase order tracking, test procedure tracking, failed asset tracking, and equipment calibration tracking.

3.1.8 Support work outside normal duty hours, as required, in order to accomplish tasking listed throughout this section.

3.1.9 Implement and track test failures and issues in the System Problem/Improvement Report (SPIR) database.

3.1.10 Provide administrative support for contracted employees who are travelling to remote locations. This includes submitting any access requests, Joint Personnel Adjudication System (JPAS) requests, country clearance requests, and other paperwork required for travel to the specific location.

3.2 Systems Engineering, Design, and Requirements: The contractor shall support the design of HM&E control systems. This includes:

3.2.1 Developing requirements for systems based on the Naval Combatant Design Specificaiton (NCDS), Design Practice Criteria (DPC) manuals, DoD and NAVSEA guidance, marine specifications, and commercial specifications as applicable

3.2.2 Performing Analysis of Alternatives (AoA) for various control system options

3.2.3 Developing technical data packages and detailed design drawings

3.2.4 Develop equipment integration designs for networking, supervisory control systems, simulators/stimulators, and other test tools/systems developed in-house.

3.2.5 Develop/modify drawings, documentation, plans and procedures for equipment integration and site upgrades

3.2.6 Develop software and hardware installation plans with input from Fleet, Type Commanders, Functional and Platform Program Managers, Planning Yards, Ship Manager Representatives (SMRs), and external supporting commands and technical authorities

3.2.7 Develop, maintain and configuration manage software and hardware installation procedures, instructions, notices and Standard Operating Procedures.

3.2.8 Develop Ship Change Documents (SCD) packages for control system deliveries.

3.2.9 Develop Engineering Change Proposal (ECP) packages for control systems.

3.2.10 Provide engineering services that include development and maintenance in support of hardware and software technical documentation and requirements.

3.2.11 Provide engineering services that include development and maintenance in support of hardware shipboard installation technical data packages (TDPs)

3.2.12 Systems Integration: The contractor shall support integration of all HM&E control systems with each other and with other shipboard systems. The contractor shall support integration efforts as follows:

3.2.12.1 Improving existing communication interfaces or develop new interfaces between control systems and new or modified ship systems.

3.2.13 Development technical documentation as it relates to control system or control system interfaces (e.g. Interface Design Documents, user manuals, training manuals, maintenance guides).

3.2.14 Review technical information on new ship systems and document impacts to control and information systems

3.2.15 Design human/machine and machine/machine interfaces to support the integration of new ship systems

3.2.16 Design and implement test tools (e.g. Sim/Stim, Emulators, Message Pumps) to support software development and integration testing of new ship systems with machinery and damage control systems.

3.2.17 Provide remote and on-site troubleshooting and root cause analysis support for other ship systems interfaced to machinery and damage control systems.

3.2.18 Design, implement, debug and test technical solutions in software (primarily C/C++, C++.net, C# and Java) to support the integration of new ship systems with machinery and damage control systems.

3.2.19 Configure and test software updates on land based test facilities in preparation for ship deliveries.

3.3 Hardware Support: The Contractor shall:

3.3.1 Develop drawings of panels, electrical circuits, and embedded electronics.

3.3.2 Provide hardware administration, maintenance, and disaster recovery support.

3.3.3 Provide staging services of all material identified as Industrial Activity Furnished (IAF) as indicated on the installation materials lists.

3.3.4 Provide temporary storage as required of Government Furnished Material (GFM) as identified by

the applicable installation documentation to be furnished as GFI.
3.3.5 Provide fabrication services for structures, mounts, materials, and other components identified by installation drawings and/or schematics.

3.4 Software Development: To ensure the readiness and safety of surface ships, NSWCPD is responsible for the software development and lifecycle support of the Future Surface Combatant HM&E control systems, both shipboard and at Land Based Engineering Site (LBES). In support of this mission, the Contractor shall:
3.4.1 Provide software lifecycle support following the NSWCPD System Engineering Process (SEP) with applicable Capability Maturity Model Integrated (CMMI) and Institute of Electrical and Electronics Engineers (IEEE) standards and specifications.
3.4.2 Develop new and modified control system computer programs from software requirements. Provide input to software team to develop requirements and desired functionality of the control system
3.4.3 Develop and/or modify computer code in the following languages: C/C++, C#, Java, Visual basic, MATLAB, and Labview as well as other related high level programming languages. The contractor shall support a range of integrated developer environments including Visual Studio, Eclipse, and Netbeans.
3.4.4 Develop and/or modify Graphical User Interfaces using applicable development tools.
3.4.5 Develop databases such as MS Access, Oracle, and SQL.
3.4.6 Develop software for embedded systems.
3.4.7 Use networked and IP-based systems and knowledge of network protocols including TCP/IP (Transmission Control Protocol/Internet Protocol) and UDP (User datagram Protocol) to develop and support communications protocols
3.4.8 Develop and/or modify network configurations
3.4.9 Develop and/or upgrade machinery plant simulations in order to enhance control system embedded trainer simulation system.
3.4.10 Develop software unit tests in order to demonstrate that the modified computer programs satisfy the requirements.
3.4.11 Develop software change packages and artifacts and present at peer reviews.
3.4.12 Use software issue reporting databases
3.4.13 Maintain technical software development skills to contribute to new software development efforts

3.5 Modeling and SIM/STIM Support: In order to reduce project risk, facilitate systems integration and improve ship system maintainability, Modeling and Simulation will be a key element in the Future Surface Combatant program and requires contracts to develop and maintain models which accurately represent the ship. The Contractor shall:
3.5.1 Research and comprehend existing Ship Systems Electrical, Mechanical and Control System designs, for the purposes of capturing essential dynamics within Matlab Simulink and potential other Simulator platforms. (RTDS, OPAL-RT)
3.5.2 Understand and leverage advanced Simulink Modeling Architectures to enable very large scale ship systems and ‘models inside models’ to effectively be developed
3.5.3 Understand concepts of Model Based Design and leverage Vendor Models within the established Navy modeling architecture
3.5.4 Develop or modify existing Models and framework to suit various needs of the Controls and Machinery Systems
3.5.5 Establish next generation Navy Simulation capabilities for hosting Electrical Networks and Controls in both non-real time and real-time
3.5.6 Develop Model Interfaces and effective ways of integrating Models with one another
3.5.7 Understand and Evaluate Simulink Solvers of both Variable and Fixed Step sizes for the purposed of Controls and Machinery
3.5.8 Understand and Develop Models for Simscape Physics Based Simulink Environment
3.5.9 Develop and enhance Simscape Custom Domains and Custom Libraries
3.5.10 Develop and Maintain Models within Simulink Projects and Repositories
3.5.11 Develop and Maintain Simulink Libraries and Components
3.5.12 Develop Model Signal Architecture and Map Connections to existing Ship Topologies
3.5.13 Understand and maintain Model I/O and interfaces to other Platform Equipment
3.5.14 Create Matlab Scripts to automate various tasks and testing needs
3.5.15 Work with Simulink Data Dictionary to Map Signal Databases to existing Ship Databases
3.5.16 Work and integrate Matlab with existing Excel and other shipboard system documentation
3.5.17 Create Test Harnesses to Verify and Validate existing Models
3.5.18 Create Simulink Dashboard and GUIs to interact with Existing Models
3.5.19 Work with and understand aspects of Speedgoat Hardware for the Real-Time execution of Simulink Models. Splitting models onto Multiple Cores etc.
3.5.20 Understand and develop models for Multi-Rate, Multi-Core and Multi-Domain execution
3.5.21 Link Models back to Documentation for tractability and requirements tracking
3.5.22 Compile and maintain Models for Real-Time testing and Lab integration
3.5.23 Understand and maintain various forms of Shipboard Controller Models (Power Systems, Protection Systems, Damage Control, PLC Stateflow based, etc)
3.5.24 Document Model capabilities, interfaces, operability and features.

3.6 Test Support: The Contractor shall:
3.6.1 Develop, plan, schedule, and execute test plans and test procedures for control system computer programs and hardware.

3.6.2 Document issues, faults, or deficiencies found during software and hardware testing. Troubleshoot issues, identify root cause and provide solutions to enable testing to continue.
3.6.3 Provide remote troubleshooting assistance to onsite control system representatives that are supporting ship light off and installation activities.
3.6.4 Provide support for the operations of the Integrated Test Facility (ITF) and Land Based Engineering Site (LBES) which is used for Future Surface Combatant testing and risk mitigation.
3.6.5 Develop software programs for use in test tools and facility infrastructure utilizing Programmable Logic Controller (PLC) ladder logic code, Python, Java, C/C++, C#, Matlab, and LabView as well as other related high level programming languages.
3.6.6 Modify existing test tool/facility infrastructure tools to implement enhanced capability based on requirements.
3.6.7 Troubleshoot in-house systems to identify root cause of problems that are found during software development and testing.

3.7 Shipboard Troubleshooting, Test, and Installation: The Contractor shall:
3.7.1 Perform shipboard software loads on Microsoft/Linux computers and processors, VxWorks processors, PLC processors and cards, and circuit level firmware.
3.7.2 Repair various shipboard hardware and electronic equipment, such as: cable harness wiring, cable harness routing, terminal box wiring, connector pinouts, wire splicing, equipment rack-in and rack-out, cable terminations.
3.7.3 Perform troubleshooting on various electronic equipment such as computer hardware, computer operating systems, computer peripherals, various electronic sensors, terminal box wiring, cable wiring, electronic circuits, contact closure devices, and mechanical/electronic switches.
3.7.4 Provide shipboard installation, troubleshooting, and test assessment plans, routine status, metrics, and final trip reports.
3.7.5 Provide support for facilitating, preparing and tracking the shipment of items to and from the waterfront.
3.7.6 Assistance with identifying drawing discrepancies, configuration issues, equipment deficiencies, and special or operational interference.
3.7.7 Troubleshoot Hull Mechanical & Electrical (HM&E) equipment to determine impact upon control system software development and maintenance.
3.7.8 Develop and maintain software and equipment installation, equipment checkout, system troubleshooting and system assessment work products. The work products shall include the following: operational and endurance parameters, testing procedures, test plans, maintenance procedures, installation procedures, operational procedures, equipment installation drawings, equipment installation requirements, equipment removal packages, troubleshooting plans, troubleshooting guides, and pass/fail criteria.
3.7.9 Provide technical and engineering support during shipboard troubleshooting of control system problems.
3.7.10 Provide installation support for various cable types, connector types, transmitters, sensors, computer systems, wiring harnesses, wiring terminal boxes, and Human Machinery Interfaces (HMI).
3.7.11 Provide shipboard operator and maintenance training of the control system.
3.7.12 Conduct control system test procedures during shipboard test evolutions.

3.8 Integrated Logistics Support (ILS) : The contractor shall:
3.8.1 Develop, evaluate, and provide feedback on technical documentation and other logistics products such as technical manuals, allowable parts lists, preventative maintenance cards, and engineering procedures
3.8.2 Provide system red-lines, drawings, equipment schematics, and damage control placards.

3.9 Cybersecurity and Information Assurance (IA). The contractor shall provide the following services:
3.9.1 Provide technical services in support of delivering cyber-secure systems and solutions including the development and submittal of Risk Management Framework (RMF) risk assessments, implementation of DoD secure system configuration and hardening, requirements identified in Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) and Security Requirements Guides (SRGs), Assured Compliance Assessment Solution (ACAS) vulnerability assessments, anti-virus (AV) scanning, Standard Engineering Process (SEP) artifacts, and other supporting documentation required for certifying and maintaining afloat, RDT&E, and/or enterprise platforms.
3.9.2 Develop RMF Assess & Authorize (A&A) package documentation in accordance with DoD/NAVSEA directives, which includes the following components: Platform IT (PIT) Determination package documentation, System Categorization Form, Information System Continuous Monitoring Strategy (ISCM), Security Plan (SP), Step Concurrence forms, Plan of Actions and Milestones (POA&M), Security Assessment Plan (SAP), Security Assessment Report (SAR), Risk Assessment Report (RAR), Security Authorization Package, CYBERSAFE Certification, Package Endorsement Letters, and any additional administrative/technical resources required for submission.
3.9.3 Ensure RMF A&A package is submitted to the certification authority (CA) in sufficient time for review and operational cybersecurity risk recommendation to obtain Designated Accrediting Authority (DAA) authorization decision prior to operations or tests on a live network (i.e. LBES or shipboard).
3.9.4 The contractor shall develop, maintain, and execute all IA related tasks and duties in accordance with regulations to include the development and execution of DIACAP/RMF Program to Plan of Action and Milestone (POA&M) or Security Technical Implementation Guide (STIG).
3.9.5 In accordance with RMF, the contractor shall monitor and maintain the security posture of IT

systems to include patching, implementing STIGs, analyzing network traffic, and applying new physical security measures such as performing offsite data storage

3.9.6 Develop and/or test new and existing security features to be implemented into the control system operating environment and/or software.

3.10 Logistics Specialist Support – Logistics Specialists shall:

3.10.1 Perform Test Plans.

3.10.2 Prepare Test Reports.

3.10.3 Perform Data Collection and Statistical Analyses.

3.10.4 Interpret Command and Department Guidance.

3.10.5 Perform financial analysis and track man-hours/time related data for engineering projects in order to track overall burn curves against project budgets, and present the cost/schedule performance metrics and data during Systems Engineering Process audits.

3.10.6 Enter shipping requests into Navy ERP (Enterprise Resource Planning).

3.11 Configuration Management Support – The contractor shall provide the following services:

3.11.1 In accordance with locally established Quality Assurance (QA) configuration control practices, the contractor shall implement and maintain proper configuration management of equipment, software, and documentation using processes compliant with Capability Maturity Model Integration (CMMI) Level 3.

3.11.2 The contractor shall implement configuration version control practices and processes (checkout/checkin, version number control, system/software baselines, merge, build, testing, and release) to software, hardware, requirements, firmware, images, technical manuals, test procedures, and support documentation.

3.11.3 The contractor shall provide configuration version control using locally established forms, templates, databases, and applications (GIT, Telelogic DOORS, Sharepoint, Excel, Word, Access, and Project)

3.11.4 The contractor shall perform configuration management of control system software and documentation in accordance with the approved SEP configuration management plan using software version control tools.

3.11.5 Maintaining configuration control of documentation and software updates from vendors and other technical departments and provide analysis of any potential impacts that updates would have on machinery and damage control systems.

3.11.6 The contractor shall provide offsite data storage at Iron Mountain (or equivalent as approved by NSWCPD Future Surface Combatant HM&E Controls Engineering Manager) facilities

3.12 Material and Asset Support

3.12.1 Support shipping of material and assets required for supporting of tasks listed herein.

3.12.2 Maintain inventory of incoming and outgoing material and assets.

3.12.3 Provide support with fabricating and assembling material and assets required for supporting of tasks listed herein, including lab and shipboard control panels.

3.12.4 Provide support with staging (drawing material from inventory in accordance with designs) of material and assets required for supporting of tasks listed herein.

3.13 General Training Support

3.13.1 Assist with development of course materials developed for machinery control and damage control systems maintenance, installation, and operation for Ship's Force, Regional Maintenance Centers, and other Naval organizations responsible for maintenance and operation of machinery and damage control systems. Assist in the running of the courses at NSWCPD facilities. Provide auditing of on-going courses and input into curriculum development.

3.13.2 Assist Government activities in classroom training and instruction.

3.13.3 Provide On-The-Job Training (OJT) for Ship's force and Regional Maintenance Center (RMC) personnel.

3.14 Surveys and Assessments

3.14.1 Provide QA inspections and installation tracking of components.

3.14.2 Conduct HM&E machinery and systems inspections and certifications when required and provide system reports (including deficiencies) to NSWCPD representative.

3.14.3 Perform system and equipment operability tests.

3.15 Obsolescence Support. The obsolescence program identifies systems that are at or near end of life and develops solutions for them. In order to support this mission, contractors shall perform the following:

3.15.1 Support obsolescence projects from identification to solution.

3.15.2 Assist in managing the business and engineering obsolescence concerns of various stakeholders.

3.15.3 Develop technical plans and solutions for obsolescence problems. Update and maintain plan as project progresses.

3.15.4 Develop solutions to difficult problems with regard to balancing cost, need date, integration into existing systems, conflicting stakeholder desires, and other factors.

3.15.5 Develop time estimates and schedules for obsolescence remediation projects, defined as a project to replace a component which has no fit/form/function replacement and requires engineering research and development activities to develop the solution, test it, field it, and update the required logistics. Update and maintain schedule as project progresses.

3.15.6 Develop budget estimates for project material and manpower needs. Update and maintain budget

as project progresses.

4. DATA REQUIREMENTS

4.1 Contract Status Report (CDRL A001)
4.1.1 This report shall reflect both prime and Subcontractor data if applicable at the same level of detail.
4.1.2 The CDRL shall be delivered electronically, unless otherwise stated, and while Contractor's format is acceptable the Government's approval must be received in writing from the COR within 5 business days before formal submission.

4.2 Travel Report (CDRL A002)
4.2.1 This report shall reflect both prime and subcontractor data if applicable at the same level of detail.
4.2.2 The CDRL shall be delivered electronically, unless otherwise stated, and while Contractor's format is acceptable, Government's approval is required from the COR.

4.3 Contractor's Personnel Roster (CDRL A003)
4.3.1 The CDRL shall be delivered electronically, unless otherwise stated, and while Contractor's format is acceptable, Government's approval is required from the COR. This report shall reflect both prime and subcontractor data if applicable at the same level of detail.

4.4 Technical Reports (CDRL A004)
4.4.1 This report shall reflect both prime and subcontractor data if applicable at the same level of detail.
4.4.2 The CDRL shall be delivered electronically, and while Contractor's format is acceptable, Government's approval is required from the COR. This report shall reflect both prime and subcontractor data if applicable at the same level of detail.

4.5 Government Property Inventory Report (CDRL A005)
4.5.1 This report shall reflect both prime and subcontractor data if applicable at the same level of detail.
4.5.2 The CDRL shall be delivered electronically, unless otherwise stated, and while Contractor's format is acceptable, Government's approval is required from the COR.

4.6 Small BusinessUtilization Report (CDRL A006)
4.6.1 This report shall reflect both prime and subcontractor data if applicable at the same level of detail.
4.6.2 The CDRL shall be delivered electronically, unless otherwise stated, and while Contractor's format is acceptable, Government's approval is required from the COR.

4.7 Systems Security Plan (CDRL A007)
4.7.1 This report shall reflect both prime and subcontractor data if applicable at the same level of detail.
4.7.2 The CDRL shall be delivered electronically, unless otherwise stated, and while Contractor's format is acceptable, Government's approval is required from the COR.
4.7.3 The CDRL shall be delivered electronically, unless otherwise stated, and while Contractor's format is acceptable, Government's approval is required from the COR.

5. SECURITY REQUIREMENTS

5.1 The Contractor is responsible for completing all required Government mandated training to maintain security and network access to government sites and IT systems to include but not limited to: Antiterrorism Level 1 Awareness; Records Management in the DON: Everyone's Responsibility; Training and Readiness: The Active Shooter; NAVSEA Introduction to Controlled Unclassified Information; Operations Security (OPSEC); NAVSEA Counterintelligence Training; Privacy and Personally Identifiable Information (PII) Awareness Training; NAVSEA Physical Security training and Cybersecurity 101 Training. Certificates of successful completion shall be sent to the COR and as otherwise specified in the contract.

5.2 In accordance with the NISPOM DoD 5220.22M, Contractor personnel that require access to Department of Navy (DON) information systems and/or work on-site require an open investigation or favorable adjudicated Tier 3 investigation by the Vetting Risk Operations Center (VROC). The investigations should be complete using the SF-86 Form and the SF-87 finger print card. Interim clearance is grant by VROC and record in the Joint Personnel Adjudication System (JPAS). An open or closed investigation with a favorable adjudication is required prior to issuance of a badge providing access to NSWCPD buildings. If an unfavorable adjudication is determined by Department of Defense Consolidation Adjudication Facility (DoD CAF) all access will be denied. For Common Access Card (CAC) you must have an open investigation and or favorable adjusted investigation. Interim security clearance are acceptable for a CAC.

5.3 Contractor personnel that require a badge to work on-site at one of the NSWCPD sites must provide an I-9 form to verify proof of citizenship. The I-9 form should be signed by the company Facility Security Officer or the company Human Resource Department. In addition to the I-9 form, Contractors shall also bring their birth certificate, current United States Passport or naturalization certificate and state issued ID to the NSWCPD Security Officer at the time of badge request to verify citizenship. Finally, contractors shall supply a copy of their OPSEC Training Certificate or other proof that the training has been completed.

5.4 Construction badges for contractor personnel that work on-site at one of the NSWCPD sites will be good for 60 days.

5.5 Vetting through the National Crime Information Center, sex offender registry, and terrorist screening database. Shall be process for any contractor that does not have a favorable adjudicated investigation in JPAS and is requesting to have a standard access control badge SACB to access NSWCPD buildings. Any contractor that has unfavorable information that was not been favorably adjudicated by DoD CAF will not be issued a badge.

5.6 Within 30 days after contract award, the Contractor shall submit a list of all Contractor personnel, including subcontractor employees, who will have access to DON information systems and/or work on-site at one of the NSWCPD sites to the appointed Contracting Officer Representative (COR) via email. The Contractor shall provide each employee's first name, last name, contract number, the NSWCPD technical code, work location, whether or not the employee has a CAC and or Standard Access Control Badge (SACB), the systems the employee can access (i.e., NMCI, RDT&E), and the name of the Contractor's local point of contact, phone number and email address. Throughout the period of performance of the contract, the Contractor shall immediately provide any updated information to the COR when any Contractor personnel changes occur including substitutions or departures.

5.7 This effort may require access to classified information up to the SECRET level. No classified data will be generated or stored by the Contractor. The Contractor is required to have and maintain a SECRET clearance. The requirements of the attached DD Form 254 apply.

5.8 The Contractor shall appoint a Facility Security Officer (FSO), who shall (1) be responsible for all security aspects of the work performed under this contract, (2) assure compliance with the National Industrial Security Program Operating Manual (NISPOM) (DOD 5220.22-M), and (3) assure compliance with any written instructions from the NSWCPD, Security Office Dorothy Morton.

5.9 The Prime Contractor shall:
5.9.1 Forward signed copies of DD254s provided to subcontractors to the Naval Surface Warfare Center Philadelphia Division (NSWCPD), ATTN: Security.
5.9.2 Direct the subcontractor to obtain approval, through the prime Contractor, for the public release of information received or generated by the sub through the prime Contractor.
5.9.3 Submit the subcontractor request for public release through the technical point of contact identified on the DD 254.

5.10 The planned utilization of non-U.S. Citizens in the performance of this contract effort must be identified by name and country of citizenship in the proposal. Foreign Nationals shall not be allowed access to classified or critical program information unless approved on a case by case basis by DSS.

5.11 The Contractor is responsible for completing all required government-mandated training to maintain security and network access to government-sites and IT systems.

5.12 The Contractor is responsible for maintaining education and certification levels respective of the designation working in the cybersecurity workforce as shown in Section 12.2 “Navy Information Assurance (IA) Workforce Requirements”.

5.13 The contract company shall ensure each employee performing shipboard work has completed the 10 hour OSHA Maritime Shipyard Employment Course #7615. The contract company shall ensure that each employee maintains a current Course #7615 certification based on the course's certification expiration period and the requirement for retraining and recertification. REF: NAVSEA SI 009-74.

6. PLACE OF PERFORMANCE

6.1 The contractor's primary place of performance shall be at government facilities in Philadelphia, PA.

6.1.1 Performance will occur at the following government sites: Building 1000, Building 77L, Building 77H, Building 4, Building 87

6.1.2 Government will provide office and lab space and phones/NMCI computers/printers for up to 18 Contractor personnel under this Contract. Note that NMCI laptops and RDT&E laptops are considered GFP.

6.1.3 The specific location(s) will be provided at time of award of the Contract. The Contractor shall provide a list of employees who require access to these areas, including standard security clearance information for each person, to the Contracting Officer Representative (COR) no later than three business days after the date of award. The work space provided to the Contractor personnel shall be identified by the Awardee, with appropriate signage listing the company name and individual Contractor employee name.

6.1.4 Access to Government buildings at Naval Surface Warfare Center Philadelphia Division is from 0600 to 1800 Monday through Friday, except Federal holidays. Normal work hours are from 0600 to 1800, Monday through Friday. Contractor employees shall be under Government oversight at all times. Government oversight requires that a Government employee be present in the same

building/facility whenever Contractor employee(s) are performing work under this Contract/Task Order. Contractor personnel are not allowed to access any Government buildings at NSWCPD outside the hours of 0600 to 1800 without the express approval of the Procuring Contracting Officer (PCO).

6.1.5 Early Dismissal and Closure of Government Facilities:

6.1.5.1 When a Government facility is closed and/or early dismissal of Federal employees is directed due to severe weather, security threat, or a facility related problem that prevents personnel from working, onsite Contractor personnel regularly assigned to work at that facility should follow the same reporting and/or departure directions given to Government personnel. The Contractor shall not direct charge to the contract for time off, but shall follow its own company policies regarding leave. Non-essential Contractor personnel, who are not required to remain at or report to the facility, shall follow their parent company policy regarding whether they should go/stay home or report to another company facility. Subsequent to an early dismissal and during periods of inclement weather, onsite Contractors should monitor radio and television announcements before departing for work to determine if the facility is closed or operating on a delayed arrival basis.

6.1.5.2 When Federal employees are excused from work due to a holiday or a special event (that is unrelated to severe weather, a security threat, or a facility related problem), on site Contractors will continue working established work hours or take leave in accordance with parent company policy. Those Contractors who take leave shall not direct charge the non-working hours to the Contract. Contractors are responsible for predetermining and disclosing their charging practices for early dismissal, delayed openings, and closings in accordance with the FAR, applicable cost accounting standards, and company policy. Contractors shall follow their disclosed charging practices during the Contract period of performance, and shall not follow any verbal directions to the contrary. The PCO will make the determination of cost allowability for time lost due to facility closure in accordance with FAR, applicable Cost Accounting Standards, and the Contractor's established accounting policy.

6.1.6 The contractor shall ensure that each contractor employee who will be resident at NSWCPD completes the Environmental Management System (EMS) Awareness training within 30 days of commencing performance at NSWCPD. This document is available at: https://navsea.navy.deps.mil/wc/pnbc-code10/Safety/default.aspx

6.1.7 In accordance with C-223-W002, ON-SITE SAFETY REQUIREMENTS (NAVSEA), the contractor shall certify by e-mail to Paul Breeden (paul.breeden@navy.mil) that on-site employees have read the “Philadelphia Division Environmental Policy and Commitment” and taken the EMS Awareness training within 30 days of commencing performance at NSWCPD. The e-mail shall include the employee name, work site, and contract number.

7. TRAVEL

7.1 The Contractor may be required to travel from the primary performance location when supporting this requirement. The estimated number of trips is 55 trips per year.

7.2 The contractor shall be required to travel CONUS (any state in USA) to accomplish the tasks contained in this contract. Travel in support of this requirement is anticipated to include, but may not be limited to, the following alternate performance locations:

ORIGIN	DESTINATION:	Number of Days Per Trip	Number of Trips	Number of People
Philadelphia, PA	Washington, D.C.	1	10	2
Philadelphia, PA	Norfolk, VA	14	5	2
Philadelphia, PA	San Diego, CA	14	10	2
Philadelphia, PA	Mayport, FL	14	5	2
Philadelphia, PA	Pascagoula, MS	14	5	2
Philadelphia, PA	Bath, ME	14	5	2
Philadelphia, PA	Orlando, FL	7	5	2
Philadelphia, PA	Annapolis, MD	7	5	2
Philadelphia, PA	Leesburg, VA	14	5	2

7.3 The number of times the Contractor may be required to travel to each location cited above may vary as program requirements dictate, provided that the total estimated travel cost is not exceeded. The numbers of trips and types of personnel traveling shall be limited to the minimum required to accomplish work requirements. All travel shall be approved by the COR before travel occurs. Approval may be via the Technical Instruction (TI). In accordance with the TI instructions, before initiating any travel the Contractor(s) shall submit a detailed and fully-burdened estimate that includes the number of employees traveling, their expected travel costs for airfare, lodging, per diem, rental car, taxi/mileage and any other costs or actions requiring approval. The travel estimate shall be submitted to the Contracting Officer's Representative (COR) and Contract Specialist. Actuals cost, resulting from the performance of travel requirements, shall be reported as part of the Contractor's monthly status report. The reportable cost shall also be traceable to the Contractor's invoice.

7.4 All travel shall be conducted in accordance with FAR 31.205-46, Travel Costs, and B-231-H001 Travel Cost (NAVSEA) and shall be pre-approved by the COR. The Contractor shall submit travel reports in accordance with DI-MGMT-81943 (CDRL A002)

7.5 Travel Costs

7.5.1 The current “maximum per diem” rates are set forth in the (i) Federal Travel Regulations for travel in the Continental United States; (ii) Joint Travel Regulations for Overseas Non-Foreign areas (e.g., Alaska, Hawaii, Guam, Puerto Rico, etc.); and (ii) Department of State (DOS) prescribed rates for foreign overseas locations.

8. GOVERNMENT FURNISHED PROPERTY

8.1 Navy Marine Corps Intranet (NMCI) Computer - The Government shall provide a NMCI computer upon successful clearance verification. Estimated delivery date is 90 days after clearance verification.

8.2 Research, Development, Test, and Evaluation (RDT&E) Computer - The Government shall provide a RDT&E computer upon successful clearance verification. Estimated delivery date is 90 days after clearance verification.

8.3 Technical Code and Contracting Officers shall only use the fillable electronic Government Furnished Property form attachment provided at http://dodprocurementtoolbox.org/site/detail/id/26 to identify GFP and include as attachments to Section J of the solicitation. See DFARS 245.103-72 and DFARS PGI 245.103-72 for further guidance.

8.4 The Contractor shall be required to acquire Privilege User Access Authority (PAA) respective of the Windows 2000/XP/7 Operating System group and the Windows 10 Operating System in accordance with Section 12.2 “ Navy Information Assurance (IA) Workforce Requirements”.

9. GOVERNMENT FURNISHED INFORMATION

9.1 GFI is for informational purposes and use by the Contractor is optional.

9.2 Technical Manuals – The Government shall supply system technical manuals 15 days after contract award. Technical manuals will be delivered digitally

10 PURCHASES

10.1 Only items directly used and incidental to the services for this Contract and for work within the scope of the Statement of Work, shall be purchased under the Other Direct Cost (ODC) line items. Purchases of an individual item that is valued above $10,000 shall be approved by the Contracting Officer prior to purchase by the Contractor. The purchase request and supporting documentation shall be submitted via email to the Contracting Officer and the Contracting Officer's Representative (COR) it shall be itemized and contain the cost or price analysis performed by the Contractor to determine the reasonableness of the pricing. Provide copies of price estimates from at least 2 vendors.

10.2 Information Technology (IT) equipment, or services must be approved by the proper approval authority. All IT requirements, regardless of dollar amount, submitted under this Contract shall be submitted to the PCO for review and approval prior to purchase. The definition of information technology is identical to that of the Clinger-Cohen Act, that is, any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. Information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

11 PERSONNEL

11.1 All persons supporting this contract as listed in the labor categories below hall, at the time of proposal submission,be U.S. citizens holding at least a current SECRET clearance, or possess a favorable DCSA adjudication as outlined in section 5.2.

11.2 Clause 52.222-2 "Payment for Overtime Premiums" will provide for the total approved dollar amount of overtime premium or will state “zero” if not approved. If overtime premium has not been approved under this contract in accordance with Clause 52.222-2, overtime effort to be performed shall be requested from the Contracting Officer prior to performance of premium overtime. For overtime premium costs to be allowable costs; the Contracting Officer is required to approve the performance of overtime prior to the actual performance of overtime. The dollar amount in FAR 52.222-2 shall equal overtime premium negotiated between the Government and the prime contractor. This overtime premium amount shall equal the prime contractor's unburdened premium OT labor costs plus the subcontractors' fully-burdened premium OT labor costs.

11.3 The level of effort for the performance of the resultant Contract is based on the following labor categories and hours per year:

Title	eCRAFT Code	GOVT-Site /KR-Site	Hours (Reg)	Hours (OT)
MANAGER, PROGRAM/PROJECT II	MANP2	KR	480	0
MANAGER, ADMINISTRATIVE II	MANA2	KR	200	0
ENGINEER, SYSTEMS II	ESY2	GOVT	1920	192
ENGINEER, SYSTEMS II	ESY2	KR	1920	192
ENGINEER, SYSTEMS IV	ESY4	GOVT	1920	192
ENGINEER, SYSTEMS IV	ESY4	KR	1920	192
ENGINEER, COMPUTER II	EC2	GOVT	3840	384
ENGINEER, COMPUTER II	EC2	KR	3840	384
ENGINEER, COMPUTER IV	EC4	GOVT	3840	384
ANALYST, FINANCIAL SYSTEMS	ANFS	GOVT	1920	192
ENGINEER, ELECTRICAL/ELECTRONICS II	EE2	GOVT	3840	384
ENGINEER, ELECTRICAL/ELECTRONICS IV	EE4	GOVT	1920	192
ENGINEER, HUMAN SYSTEM INTEGRATION II	EHSI2	GOVT	1920	192
INFORMATION SYSTEM SECURITY MANAGER II	ISSM2	KR	1920	192
INFORMATION SYSTEM SECURITY MANAGER III	ISSM3	KR	1920	192
SYSTEMS ADMINISTRATOR II	SA2	GOVT	1920	192
ELECTRICIAN, MAINTENANCE II	23182	GOVT	1920	192
FULLY QUALIFIED NAVY VALIDATOR III	FQNV3	KR	1920	192
ACQUSITION MANAGEMENT SUPPORT I	AMS1	GOVT	1920	192
ENGINEER, DESIGN II	ED2	GOVT	1920	192
SPECIALIST, CONFIGURATION MGMT I	SCM1	GOVT	1920	192
SPECIALIST, INFORMATION SYSTEM SECURITY II	SISS2	GOVT	3840	384
DRAFTER/CAD OPERATOR II	30062	KR	1920	192
LOGISTICIAN II	LGT2	KR	1920	192
MACHINIST, MAINTENANCE I (MARINE EQUIPMENT MACHINST)	23550	KR	1920	192
WAREHOUSE SPECIALIST (WAREHOUSE WORKER)	21210	KR	960	0
			55,400	5,376

11.4 Minimum Qualifications

MANAGER, PROGRAM/PROJECTII (MANP2):

Minimum Education: Bachelor's degree in Engineering or Business from an accredited college or university.

Minimum Experience: Ten (10) years of experience as a Program Manager, to include contract and sub-contract management, budgeting, scheduling, planning, estimating, and progress.

Minimum IA Workforce Baseline Certification: Refer to table in section 12, summary of the DoD 8570.01-M IA Workforce Structure Overview

ENGINEER, SYSTEMS IV (ESY4):

Minimum Education: Master of Science Degree in an Engineering discipline from an accredited college or university, or Bachelor’s Degree and 10 years' experience in the field of systems engineering

Minimum Experience: Ten (10) years of professional experience in systems engineering

Minimum IA Workforce Baseline Certification: Refer to table in section 12, summary of the DoD 8570.01-M IA Workforce Structure Overview

ENGINEER, COMPUTER IV (EC4):

Minimum Education: Master's level degree in Computer, Electrical or Electronics Engineering or Mathematics with field of concentration in computer science; or, Bachelor’s Degree in Computer or Electrical Engineering and 10 years' experience in the field of Computer or Electrical engineering and design.

Minimum Experience: Ten (10) years of professional experience in computer design, software development or computer networks

Minimum IA Workforce Baseline Certification: Refer to table in section 12, summary of the DoD 8570.01-M IA Workforce Structure Overview

ENGINEER, ELECTRICAL/ELECTRONICS IV (EE4):

Minimum Education: Master's level degree in Electrical/Electronics Engineering; or Bachelor's Degree in Electrical/Electronics Engineering and 10 years of experience in the field of electrical or electronics engineering and design

Minimum Experience: Ten (10) years of professional experience in field of electrical or electronics engineering and design

Minimum IA Workforce Baseline Certification: Refer to table in section 12, summary of the DoD 8570.01-M IA Workforce Structure Overview

INFORMATION SYSTEM SECURITY MANAGER III (ISSM3):

Minimum Education: College degree in a technical or managerial related discipline [Note: a high school diploma or HS equivalency certificate is acceptable with additional years of experience as defined in the next category].

Minimum Experience:

- Greater than five (5)* years practical experience in a Cybersecurity, Engineering, T&E or A&A (formerly C&A) related field.
- Have worked with Information Assurance tools such as DISA Enterprise Mission Assurance Support Service (eMASS), Assured Compliance Assessment Solution (ACAS) and may be required to hold a Full Security Control Assessor qualification.
- *Without college degree, greater than seven (7) years required.

Minimum IA Workforce Baseline Certification: Refer to table in section 12, summary of the DoD 8570.01-M IA Workforce Structure Overview

MANAGER, ADMINISTRATIVE II (MANA2)

Minimum Education: Bachelor's level degree in Accounting, Finance, Economics or Business Administration

Minimum Experience: Three (3) years of professional experience

Minimum IA Workforce Baseline Certification: Refer to table in section 12, summary of the DoD 8570.01-M IA

Workforce Structure Overview

ENGINEER, SYSTEMS II (ESY2)

Minimum Education: Bachelor of Science (BS) Degree in an Engineering discipline from an accredited college or university.

Minimum Experience:

- Three (3) years of professional experience in systems engineering

Minimum IA Workforce Baseline Certification: Refer to Section 11.6

ENGINEER, COMPUTER II (EC2)

Minimum Education: Bachelor's level degree in Computer, Electrical or Electronics Engineering or Mathematics with field of concentration in computer science

Minimum Experience: Three (3) years of professional experience in computer design, software development or computer networks

Minimum IA Workforce Baseline Certification: Refer to table in section 12, summary of the DoD 8570.01-M IA Workforce Structure Overview

ANALYST, FINANCIAL SYSTEMS (ANFS):

Minimum Education: Bachelor's degree in business, finance, or accounting

Minimum Experience: Three (3) years experience in a related field

Minimum IA Workforce Baseline Certification: Refer to table in section 12, summary of the DoD 8570.01-M IA Workforce Structure Overview

ENGINEER, ELECTRICAL/ELECTRONICS II (EE2)

Minimum Education: Bachelor's level degree in Electrical/Electronics Engineering

Minimum Experience: Three (3) years of professional experience in field of electrical or electronics engineering and design

Minimum IA Workforce Baseline Certification: Refer to table in section 12, summary of the DoD 8570.01-M IA Workforce Structure Overview

ENGINEER, HUMAN SYSTEM INTEGRATION II (EHSI2)

Minimum Education: Accreditation Board for Engineering and Technology (ABET) Accredited BS Degree from ABET recognized engineering curriculum.
Examples include: ME / EE / IE / CSE. OR
BS Degree in physical science, engineering, or mathematics that includes 24 semester hours in physical science and/or related engineering science such as mechanics, dynamics, properties of materials, and electronics. Examples include: Applied Math, Applied Physics, Operational Research, Modeling and Simulation, Chemistry, Biology, Computer Science, Naval Architecture.

Minimum Experience:

- 4 years of experience in Government related R&D, T&E, and systems acquisition programs.
- 4 years of relevant HSI engineering experience in at least 2 of the areas listed in the Statement of Work.

Minimum IA Workforce Baseline Certification: Refer to table in section 12, summary of the DoD 8570.01-M IA Workforce Structure Overview

INFORMATION SYSTEM SECURITY MANAGER II (ISSM2)

Minimum Education: High school diploma or HS equivalency certificate is acceptable with additional years of experience as defined in the next category).

Minimum Experience:

- 5 Years of practical experience in a Cybersecurity, Engineering, T&E or A&A (formerly C&A) related field.
- Have worked with Information Assurance tools such as DISA Enterprise Mission Assurance Support Service (eMASS), Assured Compliance Assessment Solution (ACAS) and may be required to hold an Interim Security Control Assessor qualification.

Minimum IA Workforce Baseline Certification: Refer to table in section 12, summary of the DoD 8570.01-M IA Workforce Structure Overview

SYSTEMS ADMINISTRATOR II (SA2)

Minimum Education: Bachelor’s level degree in Electrical/Electronic/Computer Engineering, Computer Science, or Information Systems

Minimum Experience: 3 years professional experience in systems administration

Minimum IA Workforce Baseline Certification: Refer to table in section 12, summary of the DoD 8570.01-M IA Workforce Structure Overview

ELECTRICIAN, MAINTENANCE II (23182)

Minimum Education: High School Diploma or Trade/Industrial School Diploma (or GED Equivalent) and/or related military training

Minimum Experience:

- Two (2) years of professional experience as an Engineering Technician
- One year of professional experience tracing signals and diagnosing or isolating cause for electrical failures
- One (1) year of professional experience reading, understanding, and interpreting electrical schematics

- One (1) year of professional experience generating write ups that detail testing performed, troubleshooting steps, and findings
- One (1) year of professional experience using a digital multimeter to conduct troubleshooting hardware systems
- One (1) year of professional experience using a personal computer to conduct troubleshooting and complete work product tasks

Minimum IA Workforce Baseline Certification: Refer to table in section 12, summary of the DoD 8570.01-M IA Workforce Structure Overview

FULLY QUALIFIED NAVY VALIDATOR III (FQNV3)

Minimum Education: Bachelor's degree in Computer Science

Minimum Experience:

- Seven (7) years of professional experience
- Qualified Navy Validator Level 3 Certification

Minimum IA Workforce Baseline Certification: Refer to table in section 12, summary of the DoD 8570.01-M IA Workforce Structure Overview

ACQUSITION MANAGEMENT SUPPORT I (AMS1)

Minimum Education: Bachelor's level degree

Minimum Experience: No required professional experience

Minimum IA Workforce Baseline Certification: Refer to table in section 12, summary of the DoD 8570.01-M IA Workforce Structure Overview

ENGINEER, DESIGN II (ED2)

Minimum Education: Bachelor's degree in an Engineering discipline or Industrial Design

Minimum Experience: Three (3) years of professional experience in mechanical, structural or electrical/electronic design

Minimum IA Workforce Baseline Certification: Refer to table in section 12, summary of the DoD 8570.01-M IA Workforce Structure Overview

SPECIALIST, CONFIGURATION MGMT I (SCM1)

Minimum Education: Bachelor's degree in an Engineering discipline or Computer Science

Minimum Experience:

- Three (3) years of professional experience in configuration management

Minimum IA Workforce Baseline Certification: Refer to table in section 12, summary of the DoD 8570.01-M IA Workforce Structure Overview

SPECIALIST, INFORMATION SYSTEM SECURITY (SISS2)

Minimum Education: Bachelor's degree in an Engineering discipline or Computer Science

Minimum Experience:

- Greater than five (5)* years practical experience in a Cybersecurity, Engineering, T&E or A&A (formerly C&A) related field
- Have worked with Information Assurance tools such as DISA Enterprise Mission Assurance Support Service (eMASS), Assured Compliance Assessment Solution (ACAS) and may be required to hold a Full Security Control Assessor qualification.

Minimum IA Workforce Baseline Certification: Refer to table in section 12, summary of the DoD 8570.01-M IA Workforce Structure Overview

DRAFTER/CAD OPERATOR II (30062)

Minimum Education: Bachelor's degree in an Engineering discipline or Associates Degree in Computer Aided Design

Minimum Experience: Five (5) year of professional experience in computer aided design.

Logistician II (LGT2)

Minimum Education: Bachelor's degree in business, systems engineering or supply chain management

Minimum Experience: Five (5) year of professional experience in logisitics or supply chain management

MACHINIST, MAINTENANCE (Marine Equipment Machinist)

Minimum Education: Apprenticeship as a marine machinist, military training programs certificate in related field, or has completed at least five (5) years of on the job training in addition to the minimum experience required below

Minimum Experience: Five (5) year of experience as a journeyman machinist working with shipboard machinery installations. Experience in performing the full range of machining operation on most types of conventional machine tools and their attachments. Experience in machining various types of metals and other materials. Experience with reading and interpreting complex blueprints and locate/extract critical dimensions and key reference points. Experience in using many types of precision measuring instruments and equipment. Must be experienced in the set-up and operation of various machine tools, such as shapers, planers, and drill presses. Experience in making alignments of work pieces and prepare work for fabrication.

WAREHOUSE SPECIALIST (WAREHOUSE WORKER) (21210)

Minimum Experience: Five (5) years of professional experience in warehousing or inventory management

12. DON Cyberspace IT (Information Technology) / Cybersecurity & Information Assurance Functions and Personnel Requirements

In accordance with DoD 8570.01-M, Information Assurance Workforce Improvement Program contractors performing IA functions must be designated as a member of the Cybersecurity\IA Workforce and meet qualification requirements for their duties, which may include both an IA baseline certification and operating system (OS)/Computing Environment (CE) certification requirement per below instructions:

1. Contractors performing Cybersecurity/IA functions must meet the minimum IA baseline certification prior to being engaged as defined in the CSWF Matrix below.
2. Contractor personnel agree as a "condition of employment" to obtain (and maintain) the appropriate certifications and continuing profession education requirements for their Cybersecurity/IAWF position.
3. Contractor personnel accessing information systems shall meet applicable training and certification requirements set forth in DoD 8570.01-M. The contractor is responsible to ensure that personnel possess and maintain the proper and current Information Assurance (IA) certifications in accordance with DoD 8570.01-M and the Computing Environment/Operating System (CE/OS) certifications in accordance with the CSWF Matrix below.
4. Upon hire all contractor personnel assigned to the IAM/IAT Level I-III position (as appropriate shall sign the Information System Privileged Access Agreement and Acknowledgement of Responsibilities statement.

Cybersecurity/IA Workforce labor categories are identified herein. The Contractor shall ensure that personnel have the proper and current information assurance certification to perform information assurance functions in accordance with DoD 8570.01-M, Information Assurance Workforce Improvement Program. The Contractor shall meet the applicable information assurance certification requirements, including:

1. DoD-approved information assurance workforce certifications appropriate for each category and level as listed in the current version of DoD 8570.01-M; and
2. Appropriate operating system certification for information assurance technical (IAT) positions as required by DoD 8570.01-M.
3. The Contractor shall provide the current information assurance certificates/documentation supporting IA certification and current status of personnel performing Cybersecurity/IA duties. Baseline and Operating System (OS) Certification requirements listed in the CSWF Matrix must be met and are a condition of hire.
4. The contractor shall ensure that cybersecurity/IA contractor personnel are appropriately certified and maintain current Continuing Professional Education (CPE) requirements as a condition of employment.
5. Contractor personnel who do not have proper and current certifications shall be denied access to DoD information systems for the purpose of performing information assurance functions.

Information assurance contractor training and certification:

1. This contract includes information assurance functional services for DoD information systems, and requires appropriately cleared contractor personnel to access a DoD information system to

perform contract duties, the contractor is responsible for providing to the contracting officer-

a. A list of information assurance functional responsibilities for DoD information systems by category (e.g., technical or management) and level (e.g., computing environment, network environment, or enclave); and
b. The information assurance training, certification, certification maintenance, and continuing education or sustainment training required for the information assurance functional responsibilities.

2. After contract award, the contractor is responsible for ensuring that the certifications and certification status of all contractor personnel performing information assurance functions as described in DoD 8570.01-M, Information Assurance Workforce Improvement Program, are in compliance with the manual and are identified, documented, and tracked.
3. The responsibilities specified apply to all DoD information assurance duties supported by a contractor, whether performed full-time or part-time as additional or embedded duties, and when using a DoD contract, or a contract or agreement administered by another agency.

Baseline Certification- The baseline certification is a security certification and is required for all IA members (all IAT and IAM levels) of the Cybersecurity Workforce/IA Workforce. Contractors must have a baseline certification prior to performing any IA duties and is a condition of hire.

Computing Environment (CE) Certification- All IAT levels require Computing Environment certification for the appropriate operating system they support and in which access is granted. These certifications are typically vendor specific and depend on the supported hardware or operating system. (i.e., Microsoft computing environment requires MCITP-SA and Linux computing environment requires LINUX+).

Continuing Professional Education (CPE) Requirements- As technology continuously advances; nearly all certifications expire or have continuing professional education (CPE) requirements. Both the baseline certifications and computing environment certifications may require continuous education. The vendor requirements state whether the certifications require continuous education.

1. Continuing Professional Education (CPE) requirements are not a direct contractor cost to the Government. The contractor is responsible for meeting the qualification requirements for all positions on the contract in the Cybersecurity/IAWF matrix and should not invoice the Government for training, certification tests, or continuing profession education requirements.

Information Assurance Functions and Personnel Requirements Note:
Ensure that if you have any labor categories that will be performing Information Assurance (IA) Requirements including contractors who will be in the Cybersecurity (CS) workforce you must identify the required security, certifications, education, and training for EACH labor category. Reference DFARS Clause 252.239-7001, DoD 8750.01-M "Information Workforce Improvement Program", and DoD 8140.01 "Cyberspace Workforce Management".

Contractor shall ensure that employees keep all required certifications current to meet Navy Information Assurance (IA) Workforce requirements. The table below is a summary of the DoD 8570.01-M IA Workforce Structure Overview as it applies for the listed cyber positions:

Position	CSWF Label**	CSWF Proficiency**	IAT or IAM Level (1,2,3)	IAWF Baseline Requirements	Operating System / Computing Environment(OS/CE) Qualification	Continuing Professional Education (CPE) Requirements	IT Level (per SECNAV M-5510.30)
Manager, Program / Project II (MANP2)	75 - Strategic Planning and Policy Development	Intermediate/Journeyman	IAM-II	CAP, GSLC, Security+ CE or Bachelor Degree from accredited University	N/A	40 CPEs Annually	IT-II
Manager, Adinistrative II (MANA2)	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Analyst, Financial Systems (ANFS)	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Acqusition Management Support I (AMS1)	N/A	N/A	N/A	N/A	N/A	N/A	N/A

Position	CSWF Label**	CSWF Proficiency**	IAT or IAM Level (1,2,3)	IAWF Baseline Requirements	Operating System / Computing Environment(OS/CE) Qualification	Continuing Professional Education (CPE) Requirements	IT Level (per SECNAV M-5510.30)
Engineer, Systems II (ESY2)	67 – Test and Evaluation	Intermediate/Journeyman	IAT-II	CCNA or CAP or Security + (CE) or Bachelor Degree from accredited University	Windows or Linux	40 CPEs Annually	IT-II
Engineer, Systems IV (ESY4)	67 – Test and Evaluation	Intermediate/Journeyman	IAT-II	CCNA or CAP or Security + (CE) or Bachelor Degree from accredited University	Windows or Linux	40 CPEs Annually	IT-II
Engineer, Computer II (EC2)	62 – Software Engineering / Development	Intermediate/Journeyman	IASAE-II	CSSLP or ECSP or SECURE C++ or Bachelor Degree from accredited University	Windows or Linux	40 CPEs Annually	IT-II
Engineer, Computer IV (EC4)	62 – Software Engineering / Development	Intermediate/Journeyman	IASAE-II	CSSLP or ECSP or SECURE C++ or Bachelor Degree from accredited University	Windows or Linux	40 CPEs Annually	IT-II
Specialist, Configuration Management I (SCM1)	62 – Software Engineering / Development	Intermediate/Journeyman	IASAE-II	CSSLP or ECSP or SECURE C++ or Bachelor Degree from accredited University	Windows or Linux	40 CPEs Annually	IT-II
Engineer, Electrical / Electronics II (EE2)	62 – Software Engineering / Development	Intermediate/Journeyman	IASAE-II	CSSLP or ECSP or SECURE C++ or Bachelor Degree from accredited University	Windows or Linux	40 CPEs Annually	IT-II
Engineer, Electrical / Electronics IV (EE4)	62 – Software Engineering / Development	Intermediate/Journeyman	IASAE-II	CSSLP or ECSP or SECURE C++ or Bachelor Degree from accredited University	Windows or Linux	40 CPEs Annually	IT-II
Engineer, Human System Integration II (EHSI2)	62 – Software Engineering / Development	Intermediate/Journeyman	IASAE-II	CSSLP or ECSP or SECURE C++ or Bachelor Degree from accredited University	Windows or Linux	40 CPEs Annually	IT-II
Engineer, Design II (ED2)	62 – Software Engineering / Development	Intermediate/Journeyman	IASAE-II	CSSLP or ECSP or SECURE C++ or Bachelor Degree from accredited University	Windows or Linux	40 CPEs Annually	IT-II
Information System Security Manager II (ISSM2)	74 – Security Program Management	Intermediate/Journeyman	IAM-II	CCNA or CAP or Security+ CE, or Bachelor Degree from accredited University	Windows or Linux	40 CPEs Annually	IT-II

Position	CSWF Label**	CSWF Proficiency**	IAT or IAM Level (1,2,3)	IAWF Baseline Requirements	Operating System / Computing Environment(OS/CE) Qualification	Continuing Professional Education (CPE) Requirements	IT Level (per SECNAV M-5510.30)
Information System Security Manager III (ISSM3)	74 – Security Program Management	Intermediate/Journeyman	IAM-II	CCNA or CAP or Security+ CE, or Bachelor Degree from accredited University	Windows or Linux	40 CPEs Annually	IT-II
System Administrator (SA2)	45 - System Administrator	Intermediate/Journeyman	IAT-II	GSEC, Security+ CE, or SSCP	MCSA Windows Server (or equivalent) or Linux+/RHCSA/RHCS Security	40 CPEs Annually	IT-II
Fully Qualified Navy Validator III (FQNV3)	74 – Security Program Management	Intermediate/Journeyman	IAM-II	CCNA or CAP or Security+ CE, or Bachelor Degree from accredited University	Windows or Linux	40 CPEs Annually	IT-II
Specialist, Information System Security (SISS2)	74 – Security Program Management	Intermediate/Journeyman	IAM-II	CCNA or CAP or Security+ CE, or Bachelor Degree from accredited University	Windows or Linux	40 CPEs Annually	IT-II
Electrician, Maintenance II (23182)	N/A	N/A	N/A	N/A	Annual Cybersecurity Awareness Training	N/A	N/A

C-202-H001 ADDITIONAL DEFINITIONS--BASIC (NAVSEA) (OCT 2018)

(a) Department - means the Department of the Navy.

(b) Commander, Naval Sea Systems Command - means the Commander of the Naval Sea Systems Command of the Department of the Navy or his duly appointed successor.

(c) References to The Federal Acquisition Regulation (FAR) - All references to the FAR in this contract shall be deemed to also reference the appropriate sections of the Defense FAR Supplement (DFARS), unless clearly indicated otherwise.

(d) National Stock Numbers - Whenever the term Federal Item Identification Number and its acronym FIIN or the term Federal Stock Number and its acronym FSN appear in the contract, order or their cited specifications and standards, the terms and acronyms shall be interpreted as National Item Identification Number (NIIN) and National Stock Number (NSN) respectively which shall be defined as follows:

(1) National Item Identification Number (NIIN). The number assigned to each approved Item Identification under the Federal Cataloging Program. It consists of nin numeric characters, the first two of which are the National Codification Bureau (NCB) Code. The remaining positions consist of a seven digit non-significant number

(2) National Stock Number (NSN). The National Stock Number (NSN) for an item of supply consists of the applicable four-position Federal Supply Class (FSC) plu applicable nine-position NIIN assigned to the item of supply.

(End of Text)

C-204-H001 USE OF NAVY SUPPORT CONTRACTORS FOR OFFICIAL CONTRACT FILES (NAVSEA) (OCT 2018)

(a) NAVSEA may use a file room management support contractor, hereinafter referred to as "the support contractor", to manage its file room, in which all official contract files, including the official file supporting this procurement, are retained. These official files may contain information that is considered a trade secret, proprietary, business sensitive or otherwise protected pursuant to law or regulation, hereinafter referred to as “protected information”. File room management services consist of any of the following: secretarial or clerical support; data entry; document reproduction, scanning, imaging, or destruction; operation, management, or maintenance of paper-based or electronic mail rooms, file rooms, or libraries; and supervision in connection with functions listed herein.

(b) The cognizant Contracting Officer will ensure that any NAVSEA contract under which these file room management services are acquired will contain a requirement that: